IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

Invicta Networks, Inc. Plaintiff, v. CrowdStrike Holdings, Inc. Defendant.	Civil Action No. 6:22-cv-277 The Honorable _____ **COMPLAINT FOR PATENT INFRINGEMENT** **JURY TRIAL DEMANDED**

COMPLAINT FOR PATENT INFRINGEMENT AND DEMAND FOR JURY TRIAL

TO THE HONORABLE JUDGE OF SAID COURT:

Plaintiff Invicta Networks, Inc. ("Invicta" or "Plaintiff"), files this Original Complaint for Patent Infringement and Damages against Defendant CrowdStrike Holdings, Inc. ("CrowdStrike" or "Defendant") and would respectfully show the Court as follows:

PARTIES

1. Plaintiff Invicta is a Delaware Corporation with its principal place of business located at 10217 Cedar Pond Drive, Vienna, VA 22182.

2. On information and belief, CrowdStrike was originally founded in 2011 and incorporated in Delaware. CrowdStrike has a principal place of business located at 206 E 9th Street, Suite 1750, Austin Texas 78701 <https://www.crowdstrike.com/blog/crowdstrike-changes-principal-executive-office-to-austin-texas/>. CrowdStrike specializes in the development and sales of security-related software and subscriptions for computers and the Internet (hereinafter referred to as "CrowdStrike Falcon Platform").

JURISDICTION AND VENUE

3. This is a civil action for patent infringement arising under the Patent Laws of the United States as set forth in 35 U.S.C. §§ 271, *et seq*.

4. This Court has federal subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a) and pendent jurisdiction over the other claims for relief asserted herein.

5. This Court has personal jurisdiction over Defendant pursuant to TEX. CIV. PRAC. & REM. CODE § 17.041 *et seq*. Personal jurisdiction exists over Defendant because Defendant has minimum contacts with this forum as a result of business regularly conducted within the State of Texas and within this judicial district, and, on information and belief, specifically as a result of, at least, committing the tort of patent infringement within Texas and this judicial district. Personal jurisdiction also exists because, on information and belief, Defendant, *inter alia*:

a. has substantial, continuous, and systematic business contacts in this judicial district;

b. owns, manages, and operates facilities within this judicial district (*e.g.*, CrowdStrike's principal executive office located at 206 E 9th Street, Suite 1750, Austin Texas 78701);

c. actively advertises to residents within this judicial district to purchase infringing products and services;

d. actively advertises to residents of this judicial district to work for CrowdStrike, <https://www.youtube.com/watch?v=rAgaI25_BUI>;

e. employs residents from this judicial district;

f. transacts business within the State of Texas;

g. operates the online university CrowdStrike University <https://www.crowdstrike.com/endpoint-security-products/crowdstrike-

university/>, which is available to and accessed by customers and potential customers of the Defendant within this judicial district;

h. continues to conduct such business in Texas through the continued operation within this judicial district; and

i. operates the Internet website, <https://www.crowdstrike.com/>, which is available to and accessed by customers and potential customers of the Defendant within this judicial district.

Accordingly, this Court's jurisdiction over the Defendant comports with the constitutional standards of fair play and substantial justice and arises directly from the Defendant's purposeful minimum contacts with the State of Texas.

6. This Court also has personal jurisdiction over the Defendant as Defendant has purposefully and voluntarily availed itself of the privilege of conducting business in the United States, the State of Texas, and specifically, this judicial district by continuously and systematically placing goods and services into the stream of commerce through an established distribution channel with the expectation that such good and services will be purchased by consumers within the United States, Texas, and this judicial district. Defendant, either directly and/or through intermediaries, uses, sells, offers to sell, distributes, advertises, and/or otherwise promotes the accused products in this judicial district. For example, CrowdStrike disclosed that it experienced a year-over-year growth of about 110%, including total revenue of $249.8 million for 2019. CrowdStrike further reported (on December 1, 2021) that its subscription program surpassed $1.5 billion in Annual Recurring Revenue, approximately 67% year-over-year subscription growth, for the third quarter of FY2022. Additional information on CrowdStrike's financial situation can be found at the following:

<https://www.sec.gov/Archives/edgar/data/1535527/000104746919003508/a2238988zs-1a.htm> and <https://ir.crowdstrike.com/news-releases/news-release-details/crowdstrike-reports-third-quarter-fiscal-year-2022-financial>.

7. On information and belief, CrowdStrike sells its products through its online website and sales representatives. Specifically, CrowdStrike claims a desire to make the Austin location the sales hub for CrowdStrike and has made it CrowdStrike's principal home. <https://www.youtube.com/watch?v=rAgaI25_BUI> and <https://www.crowdstrike.com/blog/crowdstrike-changes-principal-executive-office-to-austin-texas/>.

8. On information and belief, CrowdStrike has partnerships with many companies in the Elevate Partner Program. <https://www.crowdstrike.com/crowdstrike-elevate-partner-program/>. Many of the Partners have locations within this judicial district, including, *inter alia*: Amazon, Google, IBM Security, etc. Additionally, CrowdStrike uses its marketplace, the CrowdStrike Store, to offer partner integrations and applications to consumers.

9. Venue is proper in this Court under 28 U.S.C. §§ 1391(b), (c), (d) and 28 U.S.C. § 1400(b) based on the information and belief that the Defendant has committed and/or induced acts of infringement, and/or advertised, marketed, sold, and/or offered to sell products, including infringing products, in this judicial district, as discussed above in ¶¶ 2 and 5-8, which are incorporated by reference herein. On information and belief, and as stated above, CrowdStrike has significant ties to, and presence in, the State of Texas and the Western District of Texas, making venue in this judicial district both proper and convenient for this action.

10. By virtue of filing this Complaint, Plaintiff voluntarily consents to this Court's jurisdiction and venue.

THE PATENT-IN-SUIT

11. On March 7, 2006, United States Patent No. 7,010,698 ("the '698 patent"), entitled "Systems and Methods for Creating a Code Inspection System" was duly and legally issued by the United States Patent and Trademark Office ("USPTO") to Victor I. Sheymov, with Invicta Networks, Inc. ("Invicta") as assignee. A copy of the '698 patent is attached hereto as **Exhibit A**.

12. Plaintiff Invicta Networks, Inc., is the owner of the entire right, title, and interest in and to the '698 patent, with the right to sue in its own name.

13. The '698 patent is presumed valid under 35 U.S.C. § 282.

THE PATENTED CODE INSPECTION SYSTEM TECHNOLOGY

14. Anyone who owns a smartphone, a computer, or accesses the Internet in any way is, or should be, aware of malware – software intentionally designed to disrupt, damage, or gain unauthorized access to a computer, server, smartphone, computer network, application, or any of the many appliances/devices connected to the Internet, such as home security systems, cameras, or thermostats. Malware takes many forms, including, *inter alia*, computer viruses, worms, Trojan horses, ransomware, and spyware. The '698 patent is a seminal patent claiming systems and methods to protect computers and other devices from such malware or malicious code. The '698 patent claims priority to February 14, 2001 (at the dawn of the Internet era) and is directed to a code inspection system including a dynamic decoy system. In today's computer vernacular, such a code inspection system / dynamic decoy system may be referred to as a malware detector or a "sandbox." One of skill in the art will understand that a "sandbox" creates a separate, secure test environment, isolated from the main network or host system, in which to execute or detonate a suspicious file or web address attached to an email or a webpage, without risking harm to the host system. If the file or web address displays malicious behavior, it is deleted before being passed to

the protected host system. If the file or web address displays normal behavior, it is safely passed to the protected host system.

15. The ’698 patent overcomes shortcomings in the prior art, which could only detect previously known malicious code contained in a “library” of known code (col. 1, lines 59-67), and was ineffective and inefficient in creating and maintaining “test chambers” (decoy systems) due to the many different variations of code, malware, and operating systems (col. 2, lines 23-42). The ’698 patent addresses the need to detect and protect the host system from both known and unknown malware, by using a test chamber (a dynamic decoy system) that can be updated to mirror the current protected system or host computer (col. 3, lines 9-44 and col. 4, lines 24-35), with the test chamber simulating the protected system, including for example, the protected CPU, operating system, system memory, and all devices. By closely replicating the host or protected system, the dynamic decoy system provides users with the best evidence of how a suspected file or malicious code would behave on the host system, without risking access or harm to the host system. Such dynamic decoy systems, methods, and aspects were not well-understood, routine, or conventional at the time of the invention.

16. The ’698 patent is well-known in the cybersecurity industry. It has been cited in at least 85 patents and patent applications, including patents and patent applications filed by industry leaders, such as AT&T Corp., the International Business Machine Corp., and Microsoft Corp.

17. Claim 1 of the ’698 patent is representative of claims 7, 8, and 9, and claims, for example, a code inspection system comprising a code inspection management module, a dynamic decoy system, an actuator module, and one or more sensor modules – all of which cooperate with a protected system, while insulating the protected system from malicious code. In one embodiment, the code inspection management module monitors the protected system, while the

dynamic decoy system is updated to parallel or emulate relevant portions of the protected system. In another embodiment, the sensor modules enable the decoy system to analyze actions and results of one or more portions of the code in response to stimuli from the actuator module.

18. Claim 10 (and 19) of the ’698 patent is representative of claims 14 (and 23), 15 (and 24), 16 (and 25), and 18 (and 27), and claims, for example, information storage media and a method for creating and maintaining a dynamic decoy system based on a protected system. The claims comprise a dynamic decoy system, code that is received with the dynamic decoy system, and sensors monitoring such code within the dynamic decoy system. In one embodiment, the dynamic decoy system parallels or emulates potions of a protected system, and can be updated based on changes made to the protected system. In another embodiment, code is then introduced to the decoy system to simulate the operating conditions of the protected system and monitor actions and results.

19. Figure 3 of the ’698 patent further shows an “exemplary method for creating and maintaining a code inspection system according to this invention.” ’698 patent, 4:65-67; *see also id*., at 8:44-9:27 (explaining the exemplary steps illustrated in Figure 3). As shown in Figure 3, the dynamic decoy system, which substantially parallels the protected system (Steps 110-130), identifies malicious code (Steps 170-200), then either deletes the malicious code (Step 220, Step 250), or attempts to clean it (Steps 230-240). The malicious code is prevented from passing to and infecting the protected system with the malware (Step 260). The steps of the method, and how they operate with, or on the dynamic decoy system, its actuators, its sensors, etc., were not well-understood, routine, or conventional at the time of the invention.

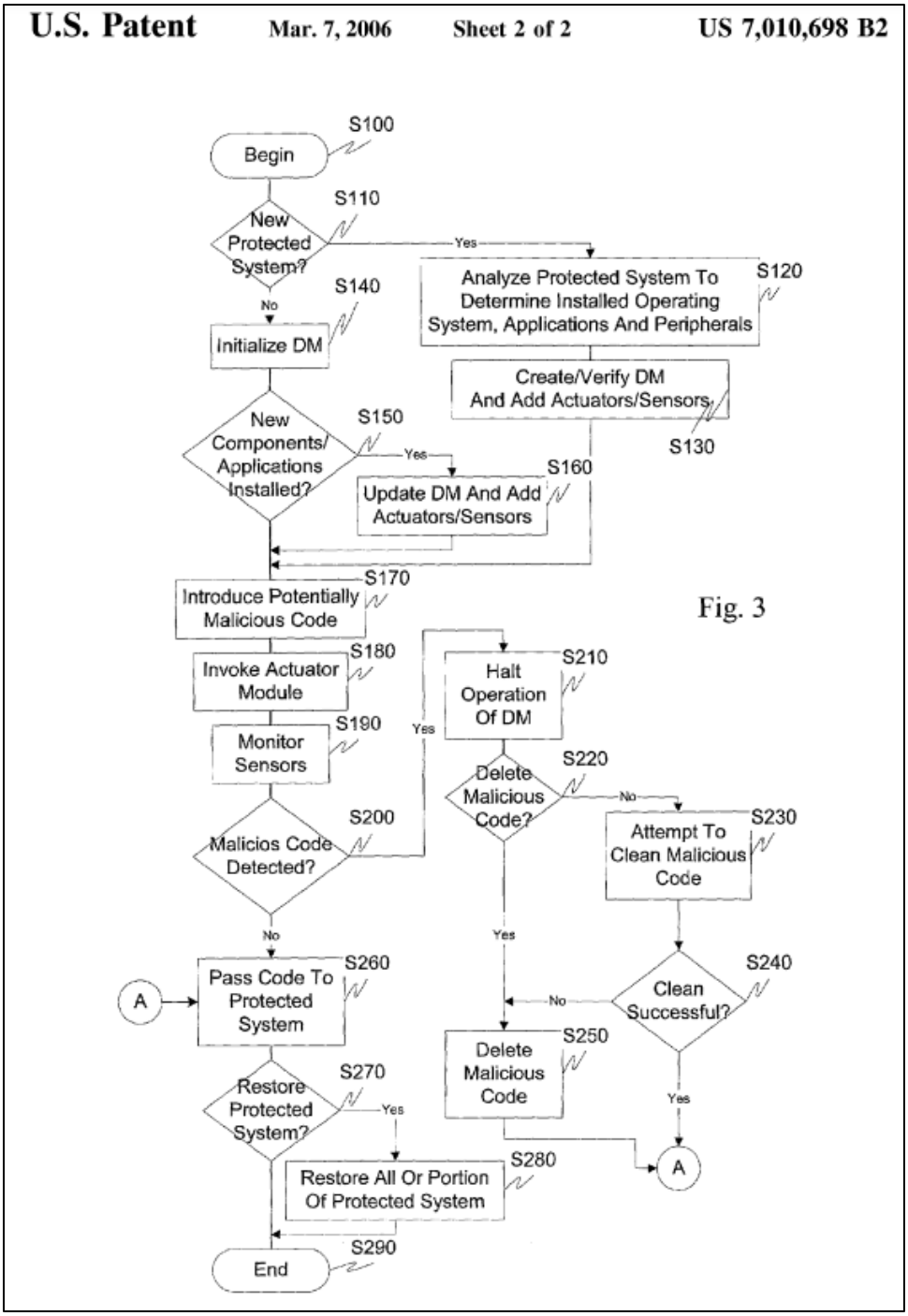
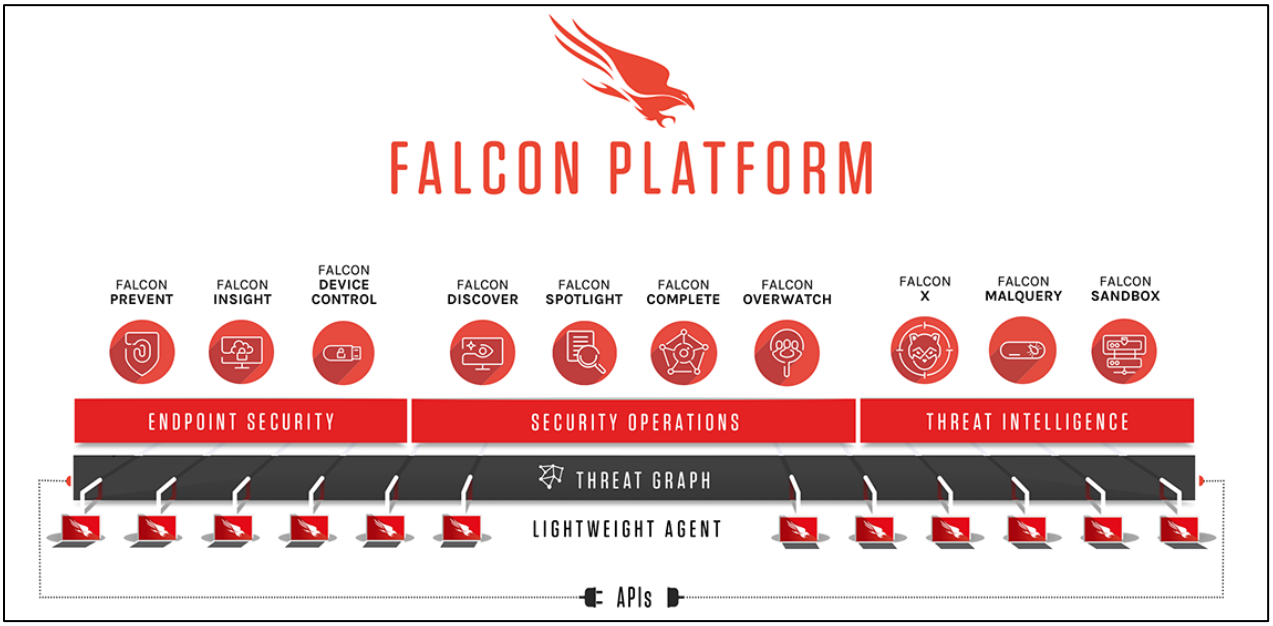


Fig. 3

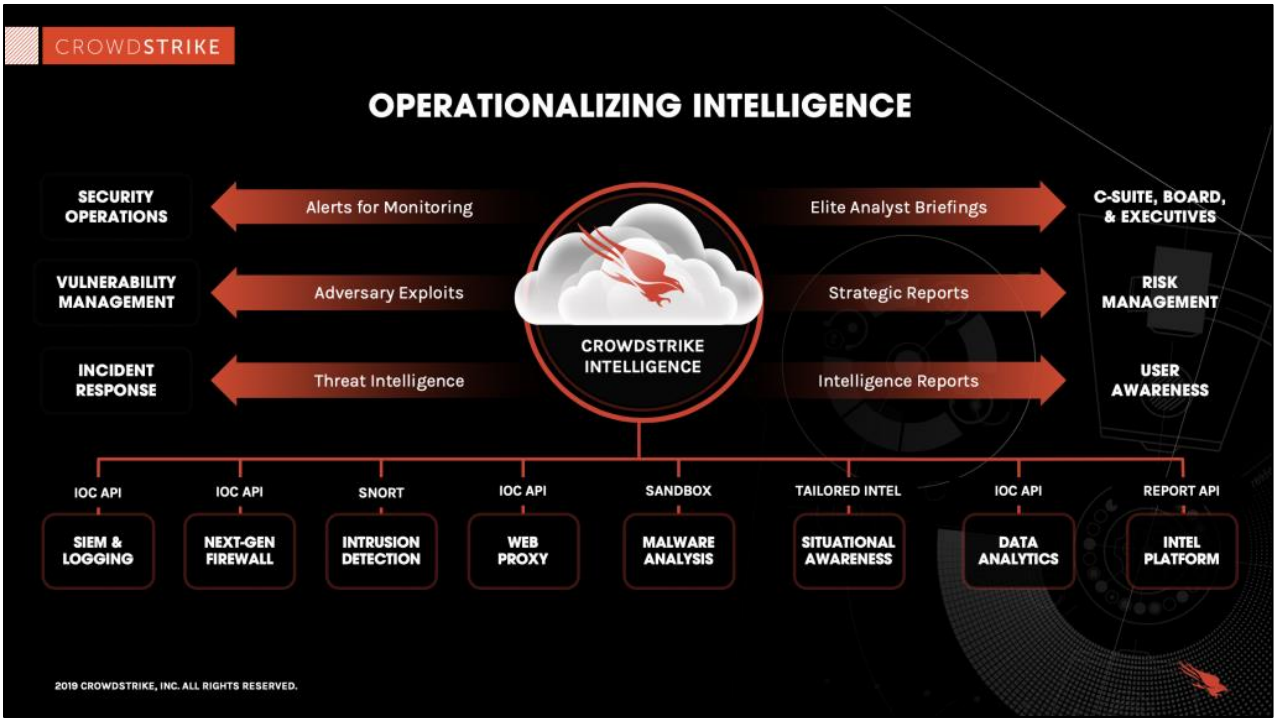
CROWDSTRIKE'S INFRINGING FALCON PLATFORM

20. On information and belief, Defendant provides endpoint security, security and IT operations, threat intelligence, and cloud security through its Falcon Platform. In particular, CrowdStrike's Falcon Platform of products and services (*e.g.*, Falcon Prevent; Falcon X; Falcon

Overwatch; Falcon Sandbox; etc.) provide – as claimed in the '698 patent – an isolation and code inspection environment that simulates portions of the hosts, such as the CPU, the operating system, system memory, and all devices, thereby infringing the '698 patent. For example, the Falcon Sandbox (*e.g.,* code inspection system) provides secure, isolated operating system environments (*e.g.*, dynamic decoy systems) that are updated to simulate or mirror a host system (*e.g.*, a protect system). Defendant's Falcon Sandbox interacts (*e.g.*, actuator modules) with the malware and observes (*e.g.*, sensor modules) every action and result.



<https://cloudprotectionworks.com/Endpoint-Protection-Platform.asp>.



<https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/>.

21. On further information and belief, Defendant's Falcon Sandbox may serve as a stand-alone module but can integrate with other CrowdStrike Falcon products (*e.g.,* Falcon Sandbox integrates with CrowdStrike's Falcon Malquery tool to compare samples with a repository of known malware), as well as CrowdStrike's partners' technologies, solutions, and services (*e.g.*, CrowdStrike's Elevate Partners). Further, and on information and belief, Defendant's Falcon Sandbox is integrated into other CrowdStrike Falcon Platform products and services (*e.g.,* Falcon X).

22. On information and belief, CrowdStrike sells the Falcon Platform as bundles: (1) Falcon Pro (https://cloudprotectionworks.com/Falcon-Pro.asp); (2) Falcon Enterprise (https://cloudprotectionworks.com/Falcon-Enterprise.asp); (3) Falcon Premium (https://cloudprotectionworks.com/Falcon-Premium.asp); and (4) Falcon Complete (https://cloudprotectionworks.com/Falcon-Complete.asp). On information and belief,

CrowdStrike also sells "Additional Falcon Modules" – Falcon Spotlight, Falcon for Mobile, and Falcon Forensics – which can be added to one of the Falcon Platform bundles. On information and belief, CrowdStrike also sells "Stand-Alone Modules" – Falcon Search Engine and Falcon Sandbox – which can be added to one of the Falcon Platform bundles or purchased on their own. And, on information and belief, CrowdStrike also sells "Specialized Products" – Falcon on GovCloud and Falcon for Data Centers – for more stringent compliance or operational requirements <https://cloudprotectionworks.com/Endpoint-Protection-Platform.asp>.

23. For the purposes of this Complaint, the term "Falcon Platform" encompasses all such code inspection and isolation functionalities and any related or integrated CrowdStrike security technologies, software, products, and services (including all products provided in bundles, sold as Additional Falcon Modules, Stand-Alone Modules, and Specialized Products).

COUNT I
INFRINGEMENT OF THE '698 PATENT

24. Plaintiff Invicta repeats and realleges the above paragraphs, which are incorporated by reference as if fully restated herein.

25. Plaintiff Invicta is the owner by assignment of all right, title, and interest in the '698 patent, including all right to recover for any and all infringement thereof.

26. Plaintiff Invicta has not licensed or otherwise authorized Defendant under the '698 patent.

27. The '698 patent is presumed valid under 35 U.S.C. § 282.

28. The '698 patent relates to, among other things, systems and methods for creating a code inspection system including a dynamic decoy system that is updated to mirror a protected host system.

29. On information and belief, Defendant has infringed the ’698 patent by making, having made, using, importing, providing, supplying, distributing, testing, selling, or offering for sale a code inspection system, as described and claimed in the ’698 patent, which simulates a host system, including for example, the protected CPU, the operating system, system memory, and all devices. For example, CrowdStrike’s Falcon Platform of products and services including CrowdStrike’s Falcon Sandbox, which is integrated into many CrowdStrike products, infringe the ’698 patent.

30. On information and belief, Defendant continues to engage in infringing acts, as described above, with knowledge of the ’698 patent by the filing of this Complaint, and with the actual intent to cause the acts which it knew or should have known would directly infringe, individually or jointly, and induce actual infringement.

Defendant’s Direct Infringement of the ’698 Patent:

31. On information and belief, in violation of 35 U.S.C. § 271(a), Defendant has directly infringed, continues to directly infringe, and will continue to directly infringe, individually or jointly, absent this Court’s intervention, one or more claims of the ’698 patent, including for example (but not limited to) at least code inspection system claims 1-9, method claims 10-18, and information storage media claims 19-27 of the ’698 patent, either literally or under the doctrine of equivalents, by making, distributing, using, testing, selling, and/or offering to sell within the United States, or importing into the United States, without license or authority, Defendant’s suite of infringing computer-security related software products, including, but not limited to, malware detection software that simulates an relevant portions of a host for isolation and inspection. For example, CrowdStrike’s Falcon Platform and such related products as provided in ¶¶ 20-23.

Direct Infringement Allegations

32. ***Direct Infringement Claim Charts:*** Exhibits 1 and 2 illustrate how CrowdStrike's Falcon Platform and related products and services perform the claimed systems, methods, and information storage media of the '698 patent. However, a person of ordinary skill in the art would readily recognize the broader implications of these representative materials.

33. On information and belief, and as demonstrated in **Exhibit 1**, Defendant CrowdStrike performs each limitation of claim 1 of the '698 patent:

> 1. A code inspection system comprising:
>
> a code inspection management module that monitors and communicates with a protected system;
>
> a dynamic decoy system that, in cooperation with the code inspection management module, is updated to substantially parallel relevant portions of the protected system;
>
> an actuator module; and
>
> one or more sensor modules, wherein the dynamic decoy system is capable of analyzing at least one of actions and results of one or more portions of code in response to stimuli from the actuator module,
>
> wherein the relevant portions of the protected system allow the one or more portions of code to be analyzed in the dynamic decoy system as if the dynamic decoy system were the protected system.

34. On information and belief, and as demonstrated in **Exhibit 1**, Defendant CrowdStrike performs each limitation of claim 7 (claim 1 is representative) of the '698 patent:

> 7. A code inspection system comprising:
>
> a code inspection management module that monitors and communicates with a protected system;
>
> a dynamic decoy system that, in cooperation with the code inspection management module, is updated to substantially parallel relevant portions of the protected system;
>
> an actuator module; and
>
> one or more sensor modules, wherein the dynamic decoy system is capable of analyzing at least one of actions and results of one or more portions of code in response to stimuli from the actuator module,
>
> wherein at least a portion of the protected system is capable of being recovered from the dynamic decoy system.

35. On information and belief, and as demonstrated in **Exhibit 1** (claim 1 is representative), Defendant CrowdStrike performs each limitation of claim 8 of the ’698 patent:

> 8. A code inspection system comprising:
> a code inspection management module that monitors and communicates with a protected system;
> a dynamic decoy system that, in cooperation with the code inspection management module, is updated to substantially parallel relevant portions of the protected system;
> an actuator module; and
> one or more sensor modules, wherein the dynamic decoy system is capable of analyzing at least one of actions and results of one or more portions of code in response to stimuli from the actuator module,
> wherein the code inspection system is an interface between the protected system and one or more unprotected systems.

36. On information and belief, and as demonstrated in **Exhibit 1** (claim 1 is representative), Defendant CrowdStrike performs each limitation of claim 9 of the ’698 patent:

> 9. A code inspection system comprising:
> a code inspection management module that monitors and communicates with a protected system;
> a dynamic decoy system that, in cooperation with the code inspection management module, is updated to substantially parallel relevant portions of the protected system;
> an actuator module; and
> one or more sensor modules, wherein the dynamic decoy system is capable of analyzing at least one of actions and results of one or more portions of code in response to stimuli from the actuator module,
> wherein the code inspection management module monitors the protected system and updates the dynamic decoy system based on at least one of installed software, installed hardware, operating system upgrades, software upgrades, hardware upgrades, software deletions, hardware deletions and input/output devices.

37. On information and belief, and as demonstrated in **Exhibit 2**, Defendant CrowdStrike performs each limitation of claim 10 of the ’698 patent:

> 10. A method of creating and maintaining a dynamic decoy system based on a protected system comprising:
> creating a dynamic decoy system that substantially parallels relevant portions of a protected system;

updating the dynamic decoy system based on changes to the protected system;

receiving one or more portions of code;

introducing the one or more portions of code to the dynamic decoy system;

simulating operating conditions of the protected system in the dynamic decoy system; and

monitoring sensors in the dynamic decoy system for at least one of actions or results of the one or more portions of code,

wherein the relevant portions of the protected system allow the one or more portions of code to be analyzed in the dynamic decoy system as if the dynamic decoy system were the protected system.

38. On information and belief, and as demonstrated in **Exhibit 2** (claim 10 is representative), Defendant CrowdStrike performs each limitation of claim 14 of the ’698 patent:

14. A method of creating and maintaining a dynamic decoy system based on a protected system comprising:

creating a dynamic decoy system that substantially parallels relevant portions of a protected system;

updating the dynamic decoy system based on changes to the protected system;

receiving one or more portions of code;

introducing the one or more portions of code to the dynamic decoy system;

simulating operating conditions of the protected system in the dynamic decoy system;

and monitoring sensors in the dynamic decoy system for at least one of actions or results of the one or more portions of code,

wherein the dynamic decoy system is an interface between the protected system and one or more unprotected systems.

39. On information and belief, and as demonstrated in **Exhibit 2** (claim 10 is representative), Defendant CrowdStrike performs each limitation of claim 15 of the ’698 patent:

15. A method of creating and maintaining a dynamic decoy system based on a protected system comprising:

creating a dynamic decoy system that substantially parallels relevant portions of a protected system;

updating the dynamic decoy system based on changes to the protected system;

receiving one or more portions of code;

introducing the one or more portions of code to the dynamic decoy system;

simulating operating conditions of the protected system in the dynamic decoy system;

monitoring sensors in the dynamic decoy system for at least one of actions or results of the one or more portions of code; and

installing one or more sensors in the dynamic decoy system that detect one or more of unauthorized access attempts, unauthorized command execution attempts and unauthorized modifications to one or more portions of the dynamic decoy machine.

40. On information and belief, and as demonstrated in **Exhibit 2** (claim 10 is representative), Defendant CrowdStrike performs each limitation of claim 16 of the ’698 patent:

16. A method of creating and maintaining a dynamic decoy system based on a protected system comprising:

creating a dynamic decoy system that substantially parallels relevant portions of a protected system;

updating the dynamic decoy system based on changes to the protected system;

receiving one or more portions of code;

introducing the one or more portions of code to the dynamic decoy system;

simulating operating conditions of the protected system in the dynamic decoy system;

monitoring sensors in the dynamic decoy system for at least one of actions or results of the one or more portions of code; and

installing an actuator in the dynamic decoy system.

41. On information and belief, and as demonstrated in **Exhibit 2** (claim 10 is representative), Defendant CrowdStrike performs each limitation of claim 18 of the ’698 patent:

18. A method of creating and maintaining a dynamic decoy system based on a protected system comprising:

creating a dynamic decoy system that substantially parallels relevant portions of a protected system;

updating the dynamic decoy system based on changes to the protected system;

receiving one or more portions of code;

introducing the one or more portions of code to the dynamic decoy system;

simulating operating conditions of the protected system in the dynamic decoy system; and

monitoring sensors in the dynamic decoy system for at least one of actions or results of the one or more portions of code,

wherein updating the dynamic decoy system is based on at least one of installed software, installed hardware, operating system upgrades, software upgrades, hardware upgrades, software deletions, hardware deletions and input/output devices.

42. The method claims and information storage media claims have similar claim language, as shown in the following independent claim pairs: 10 (19), 14 (23), 15 (24), 16 (25), and 18 (27). Plaintiff relies on **Exhibit 2** (of which claim 10 is representative), and ¶¶ 37-41 *supra*, on information and belief, as providing sufficient notice to Defendant CrowdStrike that it performs each limitation of the information storage media claims of the '698 patent.

43. On information and belief, Defendant CrowdStrike's accused products and services – CrowdStrike's Falcon Platform – embody each limitation of the dependent claims 2-6, 11-13, 17, 20-22, and 26 of the '698 patent. Reasonable discovery will confirm this interpretation. *See* **Exhibit 1** (claim 1 is representative) and **Exhibit 2** (claim 10 is representative).

Defendant's Direct Infringement of the Method Claims

44. Defendant performs the methods recited in claims 10-18 of the '698 patent. Infringement of a method claim requires performing every step of the claimed method. Defendant performs every step of the methods recited in claims 10-18. As set forth above, Defendant performs, for example, the method recited in claim 10, *i.e.*, "10. A method of creating and maintaining a dynamic decoy system based on a protected system comprising: creating a dynamic decoy system that substantially parallels relevant portions of a protected system; updating the dynamic decoy system based on changes to the protected system; receiving one or more portions of code; introducing the one or more portions of code to the dynamic decoy system; simulating operating conditions of the protected system in the dynamic decoy system; and monitoring sensors in the dynamic decoy system for at least one of actions or results of the one or more portions of code, wherein the relevant portions of the protected system allow the one or more portions of code to be analyzed in the dynamic decoy system as if the dynamic decoy system were the protected system."

45. Even if one or more steps recited in method claims 10-18 are performed through technologies not in the physical possession of the Defendant (*e.g.*, in the possession of CrowdStrike's partners, end-users, etc.), the claimed methods are specifically performed by CrowdStrike's products and services, such as CrowdStrike's Falcon Platform (*e.g.*, Falcon Sandbox). Defendant directly infringes as its products and service – CrowdStrike's Falcon Platform – dictate the performance of the claimed steps, such as the "creating," "updating," "receiving," "simulating," and "monitoring" steps recited in claim 10 of the '698 patent. Defendant's products and services are designed and built by Defendant to perform the claimed steps automatically. On information and belief, only Defendant can modify the functionality relating to these activities; no one else can modify such functionality. Defendant therefore performs all of the claimed steps and directly infringe the asserted method claims of the '698 patent, as demonstrated in **Exhibit 2.**

46. ***Additionally or alternatively***, to the extent third parties or end-users perform one or more steps of the methods recited in claims 10-18 of the '698 patent, any such action by third parties and/or end-users is attributable to Defendant, such that Defendant is liable for directly infringing such claims in a multiple actor or joint infringement situation, because Defendant directs or controls the other actor(s). In this regard, Defendant conditions participation in activities, as well as the receipt of benefits, upon performance of any such step by any such third party or end-user. Defendant exercises control over the methods performed by its products and services – for example CrowdStrike's Falcon Platform (*e.g.*, Falcon Sandbox) – and benefits from others' use, including, without limitation, creating and receiving ongoing revenue streams from the accused products and related goods, and improvement/enhancement of its products and services. End-users and third parties receive a benefit from fiscal gains (*e.g.*, partners increasing the value of their own

products through use of the CrowdStrike store and CrowdStrike's products and services) and enhanced cybersecurity (*e.g.*, end-users and third parties are protected from malware or malicious code). Such security forms the basis of entire businesses, such as those listed above as CrowdStrike partners. Defendant also establishes the manner and timing of that performance by the third-party or end-user, as dictated by the claimed method steps. All third-party and end-user involvement, if any, is incidental, ancillary, or contractual.

47. Thus, to the extent that any step of the asserted method claims is performed by someone other than Defendant (*e.g.*, an end-user or third party), Defendant nonetheless directly infringes the '698 patent at least by one or more of: (1) providing products and services, for example CrowdStrike's Falcon Platform, built and designed to perform methods covered by the asserted method claims; (2) dictating via software and associated directions and instructions (*e.g.*, to end-users) the use of the accused products such that, when used as built and designed by Defendant, such products perform the claimed methods; (3) having the ability to terminate others' access to and use of the accused products and related goods and services if the accused products are not used in accordance with Defendant's required terms; (4) marketing and advertising the accused products, and otherwise instructing and directing the use of the accused products in ways covered by the asserted method claims; and (5) updating and providing ongoing support and maintenance for the accused products.

Defendant's Direct Infringement of the System and Information Storage Media Claims

48. Defendant makes, uses, sells, offers to sell, and/or imports the code inspection systems recited in claims 1-9 and the information storage medias recited in claims 19-27. Such claims are infringed when an accused system or media, having every element of the claimed system or media, is made, used, sold, offered for sale, or imported within the United States. Defendant

makes, uses, sells, offers to sell, and/or imports the accused products (or causes such acts to be performed on its behalf), which possess every element recited in claims 1-9 and 19-27, as set forth in more detail above and demonstrated in **Exhibit 1** and **Exhibit 2** attached. Defendant therefore directly infringes the system and media claims of the ’698 patent.

49. ***Additionally or alternatively,*** regarding any “use” of the accused systems “by customers,” which is a subset of the direct infringement of system claims, Defendant directly infringes in such situations, as Defendant puts the accused products and services into service and, at the same time, controls the system as a whole and benefits from it. Defendant provides all components in the system and controls all aspects of its functionality. Although third parties (*e.g.*, CrowdStrike partners, etc.) and end-users (*e.g.*, customers.) may have physical control over certain aspects of the accused systems, Defendant retains control over how the accused system operates (*e.g.*, by having built and designed its products and services, for example, CrowdStrike’s Falcon Platform, including the Falcon Sandbox, to automatically inspect and analyze potentially malicious code (and similar data) in a particular, non-modifiable manner). The nature and extent of Defendant’s control over the system, and the benefits realized from each element of the claims, was discussed above in connection with the asserted method claims. Such discussion is incorporated herein by reference. Defendant collects valuable data through its control of this system, which in turn is used to optimize, improve, and enhance CrowdStrike’s systems, products, services, etc. as a whole – again benefitting Defendant.

50. ***In the alternative,*** if the end-user or third-party is deemed to put the invention into service and controls the system as a whole, the end-user and third-party benefit from each element of the claims because Defendant’s products and services (*e.g.*, CrowdStrike’s Falcon Platform) are designed and built by Defendant to perform the claimed steps automatically. End-users receive a

benefit from putting the invention into service, thereby protecting their personal or business computer systems, networks, etc., from possible cyberattacks and malware. Third parties (*e.g.*, CrowdStrike's partners, etc.) receive a benefit from putting the invention into service by improving their own products and services, which improves their own profits. Further, and on information and belief, third-party partners share a fiscally/contractually beneficial relationship with CrowdStrike. In both cases, CrowdStrike would be liable as an inducing infringer as described below.

Induced Infringement

51. Defendant has induced and will continue to induce others' infringement of claims 1-27 of the '698 patent, in violation of 35 U.S.C. § 271(b). As of the date of this filing, Defendant has actively encouraged infringement of the '698 patent, knowing that the acts it induced constituted infringement of the '698 patent, and its encouraging acts actually resulted in direct patent infringement by others.

52. On information and belief, Defendant has and continues to promote, advertise, and support end-users (*e.g.,* customers) and third parties (*e.g.*, CrowdStrike's partners) of its Falcon Platform, with actions to include, but not limited to the following:

(i) Defendant advertises CrowdStrike Falcon, for example its Falcon Sandbox, on its website <https://www.crowdstrike.com/endpoint-security-products/falcon-sandbox-malware-analysis/>;

(ii) Defendant provides data sheets, video demonstrations, blog posts, podcast, white papers and webinars to potential customers from its website <https://www.crowdstrike.com/wp-content/uploads/2020/03/FalconXSandboxDatasheet.pdf>,

<https://www.crowdstrike.com/resources/videos/falcon-sandbox-demo/>, <https://www.crowdstrike.com/blog/leveraging-falcon-sandbox-to-detect-and-analyze-malicious-pdfs-containing-zero-day-exploits/>, <https://www.crowdstrike.com/resources/white-papers/>; <https://www.crowdstrike.com/endpoint-security-products/falcon-sandbox-malware-analysis/>.

(iii) Defendant provides an educational course at CrowdStrike University to potential users and partners. <https://www.crowdstrike.com/resources/data-sheets/crowdstrike-university-cst-350-syllabus/>.

(iv) Defendant provides free trials for CrowdStrike Falcon products, for example, its Falcon Sandbox, on its website <https://go.crowdstrike.com/HybridAnalysisRequest.html>.

(v) Defendant provides an extensive partner program for supporting the software <https://www.crowdstrike.com/crowdstrike-elevate-partner-program/>;

(vi) Defendant offers partner integrations through the CrowdStrike store, including at least integrations from: Proofpoint, ServiceNow, Okta, Netskope, Mimecast, Zscaler, Google Cloud, Amazon Web Services, Cloudflare, Medigate, Claroty, Exabeam, Splunk, SumoLogic, IBM Security, Securonix, Akami, Awake Security, Vectra, Aruba, CyberArk, ForgeRock, ThreatWarrior, and SecureCircle. <https://store.crowdstrike.com/collection/partner-integrations>.

On information and belief, Defendant controls the distribution and implementation of its CrowdStrike Falcon Platform products and services. On information and belief, Defendant continues to engage in these acts with knowledge of the ’698 patent by the filing of this Complaint,

and with the actual intent to cause the acts which it knew or should have known would induce actual infringement.

Damage to Invicta Networks Inc.

53. Defendant CrowdStrike has infringed the ’698 patent by making, having made, using, importing, providing, supplying, distributing, testing, selling, or offering for sale code inspection systems utilizing methods for creating and maintaining a dynamic decoy system, and related information storage media.

54. On information and belief, Defendant’s actions have and continue to constitute active inducing infringement of at least code inspection system claims 1-9, method claims 10-18, and information storage media claims 19-27 of the ’698 patent in violation of 35 U.S.C. §271(b).

55. As a result of Defendant’s infringement of at least code inspection system claims 1-9, method claims 10-18, and information storage media claims 19-27 of the ’698 patent, Plaintiff Invicta has suffered monetary damages in an amount yet to be determined, in no event less than a reasonable royalty, and will continue to suffer damages in the future unless Defendant’s infringing activities are enjoined by this Court.

56. Defendant’s wrongful acts have damaged and will continue to damage Plaintiff Invicta irreparably, and Plaintiff has no adequate remedy at law for those wrongs and injuries. In addition to its actual damages, Plaintiff Invicta is entitled to a permanent injunction restraining and enjoining Defendant and its agents, servants, and employees, and all persons acting thereunder, in concert with, or on its behalf, from infringing at least code inspection system claims 1-9, method claims 10-18, and information storage media claims 19-27 of the ’698 patent.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Invicta respectfully requests that this Court enter:

A. A judgment in favor of Plaintiff Invicta that Defendant has been and is infringing at least claims 1-27 of the ’698 patent pursuant to 35 U.S.C. §§ 271(a) and/or 271(b);

B. A permanent injunction enjoining Defendant and its officers, directors, agents, servants, affiliates, employees, divisions, branches, subsidiaries, parents, and all others acting in concert or privity with any of them from infringing, or inducing the infringement of, at least claims 1-27 of the ’698 patent;

C. A judgment awarding Plaintiff Invicta all damages adequate to compensate it for Defendant’s infringement of the ’698 patent under 35 U.S.C. § 284, and in no event less than a reasonable royalty for Defendant’s acts of infringement, including all pre-judgement and post-judgment interest at the maximum rate permitted by law, and also any past damages permitted under 35 U.S.C. § 286, as a result of Defendant’s infringement of at least at least claims 1-27 of the ’698 patent;

D. An assessment of costs, including reasonable attorney fees pursuant to 35 U.S.C. § 285, prejudgment, and post judgment interest against Defendant; and

E. Any other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Pursuant to FED. R. CIV. P. 38, Plaintiff Invicta hereby demands a trial by jury on all issues so triable.

Dated: March 15, 2022

Respectfully submitted,

By: __*/s/ Thomas M. Dunlap*_____
Thomas M. Dunlap (Admitted W.D. Tex./
VA Bar No. 44016)
DUNLAP BENNETT & LUDWIG PLLC
8300 Boone Blvd., Suite 550
Vienna, Virginia 22182

Telephone: (703) 777-7319
Fax: (703) 777-3656
Email: tdunlap@dbllawyers.com

Brian Medich (Admitted W.D. Tex./
D.C. Bar No. 1671486)
DUNLAP BENNETT & LUDWIG PLLC
1200 G St. NW, Suite 800
Washington, D.C. 20005
Telephone: (571) 919-6734
Fax: (855) 226-8791
Email: bmedich@dbllawyers.com

Raymond Jones*
DUNLAP BENNETT & LUDWIG PLLC
211 Church St. SE
Leesburg, VA 20175
Telephone: (703) 777-7319
Fax: (855) 226-8791
Email: rjones@dbllawyers.com

** Application to appear Pro Hac Vice Forthcoming*

Attorneys for Invicta Networks, Inc.